| Subject Title: **Introduction to IoT** | | | | | | |
|---|---|---|---|---|---|---|
| **Course Code: PE3101** | **Year and Semester: III – I** | | L | T | P | C |
| **Prerequisites: Computer Networks, Microcontroller basic** | | | 3 | 0 | 0 | 3 |

**Unit–1: Introduction** **10 hrs**

Definition and Characteristics of IoT – IoT Architectures-Challenges and Issues - Physical Design of IoT, Logical Design of IoT - IoT Functional Blocks, Security.

---

**History of IOT**

1999- The term "Internet of Things" was used by Kevin Ashton during his work at P&G which became widely accepted

2004 - The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American

2005-UN's International Telecommunications Union (ITU) published its first report on this topic.

2008- The Internet of Things was born

2011- Gartner, the market research company, include "The Internet of Things" technology in their research

**What is the internet of things (IoT)?**

"The Internet of Things (IoT) is a system of interrelate computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

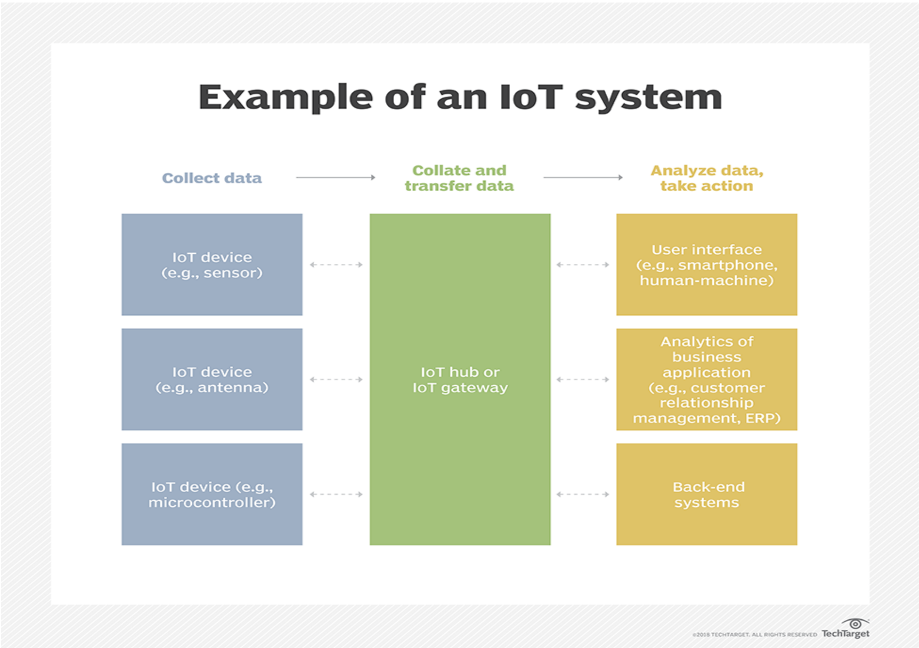
The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

**How does IoT work?**

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data



.

**Few Applications of IoT**

- ✓ Building and Home automation
- ✓ Manufacturing
- ✓ Medical and Healthcare systems
- ✓ Media
- ✓ Environmental monitoring
- ✓ Infrastructure management
- ✓ Energy management
- ✓ Transportation
- ✓ Better quality of life for elderly

---

**IoT Definitions**

- The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances. (Wikipedia)

- The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects. (IoT 2008)

- “Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”. (IoT in 2020)

## Characteristics of Internet of Things

According to the definition of internet of things (IoT), there are lot of IoT devices which are interconnected with each through internet. These devices sense the data continuously from their environment. Sensed data can either share with each other or transmitted on cloud server.

IoT has various characteristics but most common are explained under, **Major Characteristics of the Internet of Things**

The characteristics of IoT is described as follows.

**1. Connectivity**

Connectivity is an important pillar of the IoT infrastructure. IoT devices should be connected regardless of their presence. Without connection, nothing makes sense.

**2. Identity**

Each IoT device has its unique identity. If it needs to access the data from specific device then its identification element is very helpful.

**3. Intelligence**

The extraction of data from the sensor devices is very important. This data is only useful if it is interpreted properly. IoT perform operations on sensed data in such a way that the results are useful for us. It is the intelligence property of IoT.

**4. Scalability**

The number of IoT devices are increasing day by day. Hence, the scalability of an IoT should be enough that it can handle the massive traffic.

**5. Dynamic and Self-Adapting**

IoT devices should dynamically adapt themselves according to situations. For example, a camera can capture data according to light conditions. It is shifted to night or day mode automatically. It is self-Adapting technique

**6. Architecture**

IoT architecture should be hybrid, supporting different manufacturers. So, it cannot be homogeneous in nature. IoT is not the name of any engineering branch. IoT comes to picture when multiple domains come together.

**7. Safety**

Safety should be the top priority. But in case of IoT, Safety is big challenge because multiple things are connected through internet. And security at each node is a critical and tough task.

---

## Architecture of Internet of Things (IoT)

Internet of Things (IoT) technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

**3 layer IoT architecture :**

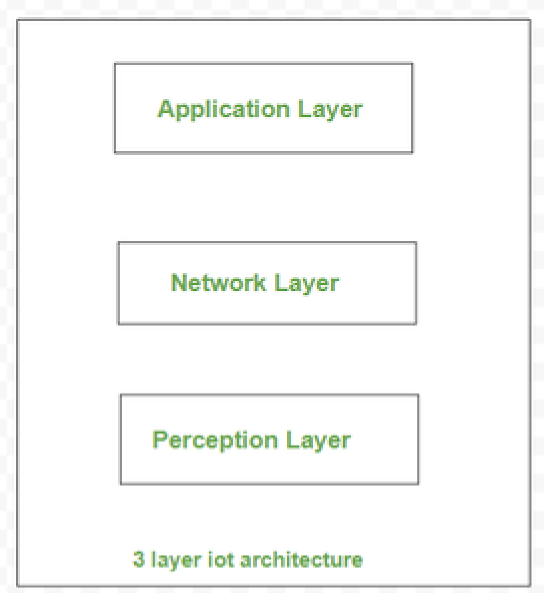



*Fig: 3 layer iot architecture*

A three-layer architecture is the common and generally known structure. It was first used in the initial phases of this IoT study. It indicates three levels: perception, network, and application.

**1. Perception Layer :**

This perception layer is the IoT architecture's physical layer. In these sensors and embedded systems are used mainly. These collect large amounts of data based on the requirements. This also includes edge devices, sensors, and actuators that communicate with the surroundings. It detects certain spatial parameters or detects other intelligent things /objects in the surroundings.

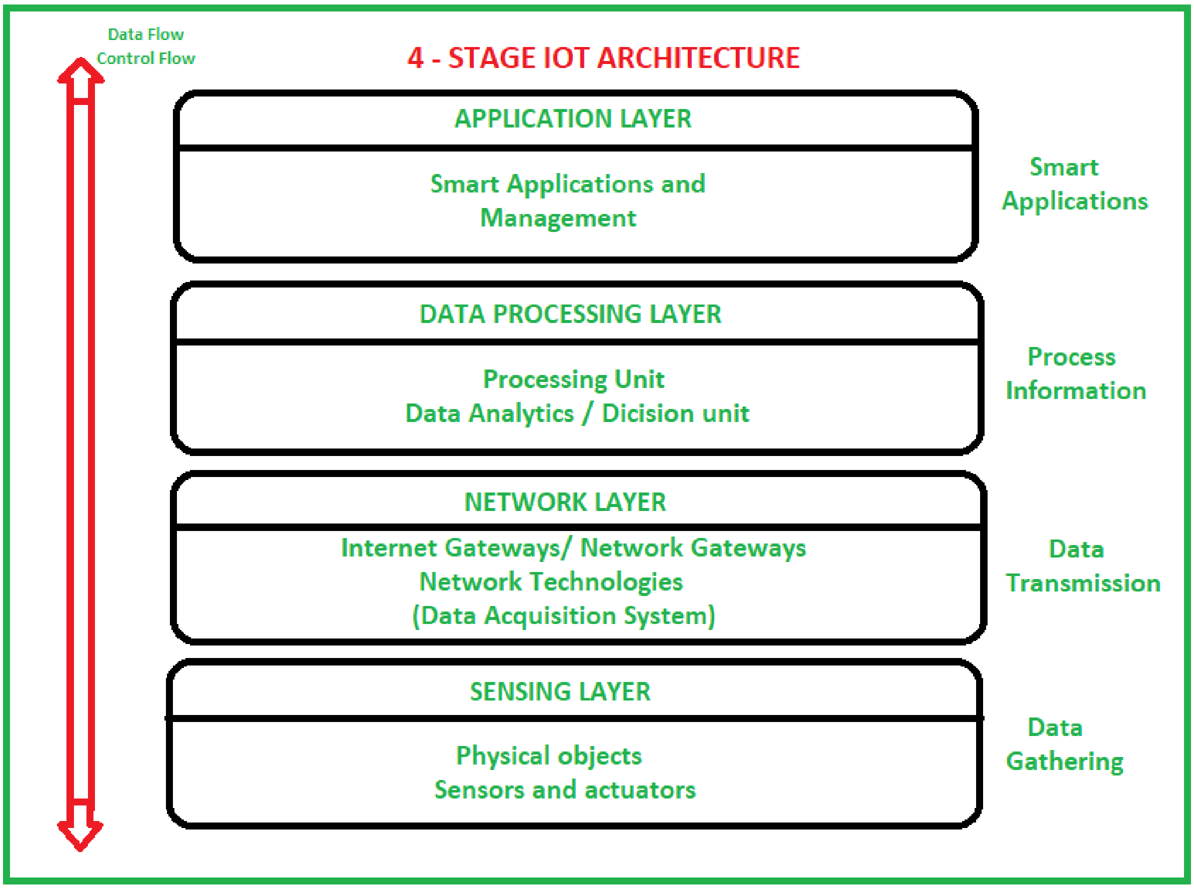
**2. Network Layer :**

The data obtained by these devices must be distributed and stored. This is the responsibility of the network layer. It binds these intelligent objects to other intelligent/ smart objects. It is also in charge of data transfer. The network layer is in-charge of linking smart objects, network devices, and servers. Its is also used to distribute and analyze sensor data.

**3. Application Layer :**

The user communicates with this application layer. It is in-charge of providing the customer with software resources. Example: in smart home application, where users press a button in the app to switch on a coffee machine, for example. The application layer is in-charge of providing the customer with application-specific resources. It specifies different uses for the IoT, such as smart houses, smart cities, and smart health.

**Four Layered IoT architecture.**

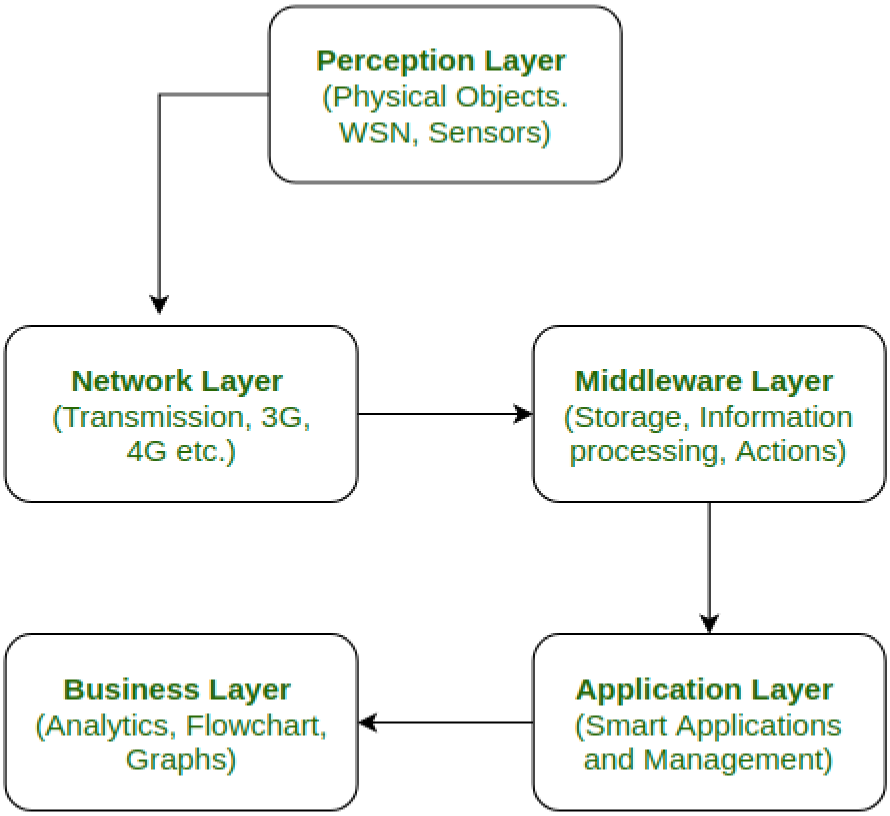



So, from the above image it is clear that there is 4 layers are present that can be divided as follows: Sensing Layer, Network Layer, Data processing Layer, and Application Layer.
These are explained as following below.

1. **Sensing Layer –**
   Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data (physical/environmental parameters), processes data and emits data over network.
2. **Network Layer –**
   Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc). Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also some times decision making based on inputted data and data management services, etc.

3. **Data processing Layer –**
   This is processing unit of IoT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored, and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.
4. **Application Layer –**
   This is last layer of 4 stages of IoT architecture. Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

**5 Layer Architecture of IoT:**
When project work is done with various cutting-edge technologies and broad application area, 5-layer architecture is considered as best. 5 Layer model can be considered as an extension to the basic architecture of IoT because it has two additional layers to the basic model.




**5 Layer Architecture of Internet of Things**

- **Perception Layer :**
  This is the first layer of IoT architecture. In the perception layer, number of sensors and actuators are used to gather useful information like temperature, moisture content, intruder detection, sounds, etc. The main function of this layer is to get information from surroundings and to pass

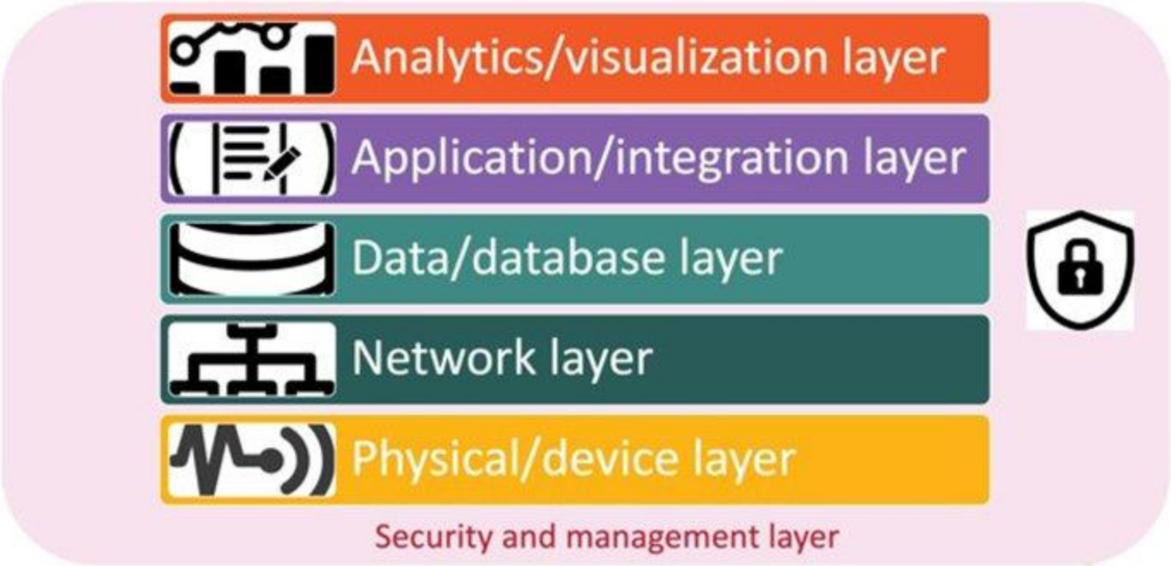
data to another layer so that some actions can be done based on that information.

- **Network Layer :**
  As the name suggests, it is the connecting layer between perception and middleware layer. It gets data from perception layer and passes data to middleware layer using networking technologies like 3G, 4G, UTMS, WiFI, infrared, etc. This is also called communication layer because it is responsible for communication between perception and middleware layer. All the transfer of data done securely keeping the obtained data confidential.
- **Middleware Layer:**
  Middleware Layer has some advanced features like storage, computation, processing, action taking capabilities. It stores all dataset and based on the device address and name it gives appropriate data to that device. It can also take decisions based on calculations done on dataset obtained from sensors.
- **Application Layer:**
  The application layer manages all application process based on information obtained from middleware layer. This application involves sending emails, activating alarm, security system, turn on or off a device, smartwatch, smart agriculture, etc.
- **Business Layer:**
  The success of any device does not depend only on technologies used in it but also how it is being delivered to its consumers. Business layer does these tasks for the device. It involves making flowcharts, graphs, analysis of results, and how device can be improved, etc.

**Six Layered IoT architecture**

The six layers of IoT architecture as described below.

Note that in some cases, layers are made up of sublayers. This a common characteristic in complex architectures, such as that of IoT.




1. **Physical/device layer.** This comprises the sensors, actuators and other smart devices and connected devices that comprise the physical layer and device layer. These smart devices either capture data (sensors), take action (actuators) or sometimes both.

2. **Network layer.** This comprises the network devices and communications types and protocols (5G, Wi-Fi, Bluetooth, etc.). Although many IoT architectures rely on general-purpose network layers, there is an increasing trend to move to dedicated IoT-specific networks.

3. **Data/database layer.** This also includes the database platform layer. There are a range of databases used for IoT architectures, and many organizations spend a fair amount of time selecting and architecting the right IoT databases.

4. **Analytics/visualization layer.** This layer comprises the analytics layer, visualization layer and perception layer. In essence, this layer's focus is on analyzing the data provided by IoT and providing it to users and applications to make sense of.

5. **Application/integration layer.** This is the layer of applications and platforms that integrate together to deliver the functionality from the IoT infrastructure to the business. In other words, the application layer, platform layer and integration layer are what provide the business value from the IoT infrastructure. The processing layer and business layer are all part of the larger application/ integration layer.

6. **Security and management layer.** As the name implies, this layer encompasses both the security layer and the management layer. Strictly speaking, this is not a *layer* as it has connections with all the other layers to provide security and management. But it's an important component that's worth considering at every layer.

---

**CHALLENGES AND ISSUES**

The main challenges and issues in IOT are

- Mobility
- Reliability
- Scalability
- Management
- Availability
- Interoperability

**Mobility:**

Most of the IoT devices are mobile and hence they have a dynamic topology. Their IP address change based on the network and location. Routing protocols need to be adaptive to the changes in the network topology. If the mobility results in change of the service provider, the complexity further increases.

**Reliability:**

IoT applications require devices to be more reliable and should respond to the changing environment rapidly and should communicate reliably. This is very crucial as a wrong information can lead to disastrous scenarios.

**Scalability:**

The scalability is the biggest challenge in IoT network. As the number of connected devices in the network increases, managing the devices and their distribution becomes difficult. Accommodating services to the newly joined devices is also a tedious task.

**Management:**

Management involves Faults, Configuration, Accounting, Performance and Security (FCAPS)aspects of all the devices.

**Availability:**

Availability is another factor of prime importance. The device should be available both in terms of software (services provided) and hardware (accessibility to other devices, compatibility with existing IoT functionalities and protocols)

**Interoperability:**

Heterogeneity is the key attribute to the IoT network. With devices with different hardware platforms, operating systems, interoperability is the major issue of concern in IoT.

---

**Physical Design of Internet of Things (IOT)**

The physical design of an IoT system is referred to as the Things/Devices and protocols that are used to build an IoT system. all these things/Devices are called Node Devices and every device has a unique identity that performs remote sensing, actuating and monitoring work. and the protocols that are used to establish communication between the Node devices and servers over the internet.

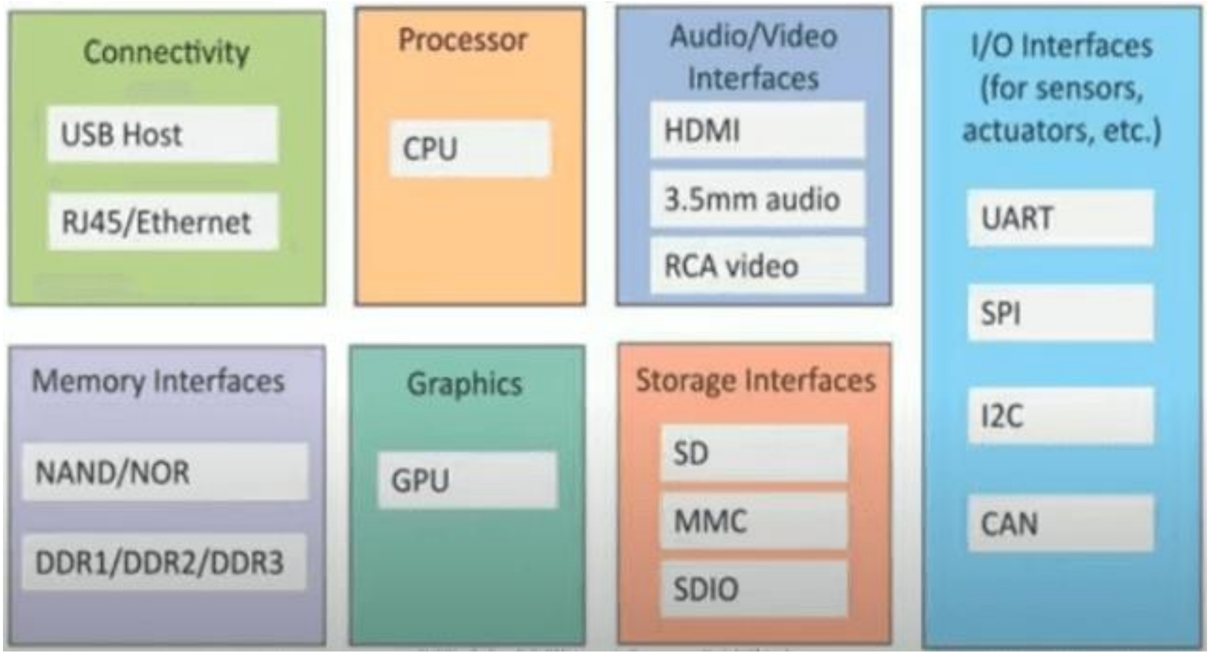
**Physical Design of IoT**

# Physical Design of IoT


**Things/Devices**

Things/Devices are used to build a connection, process data, provide interfaces, provide storage, and provide graphics interfaces in an IoT system. all these generate data in a form that can be analyzed by an analytical system and program to perform operations and used to improve the system.

for example temperature sensor that is used to analyze the temperature generates the data from a location and is then determined by algorithms.



**Connectivity**

Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

**Processor**

A processor like a CPU and other units are used to process the data. these data are further used to improve the decision quality of an IoT system.

**Audio/Video Interfaces**

An interface like HDMI and RCA devices is used to record audio and videos in a system.

**Input/Output interface**

To give input and output signals to sensors, and actuators we use things like UART, SPI, CAN, etc.

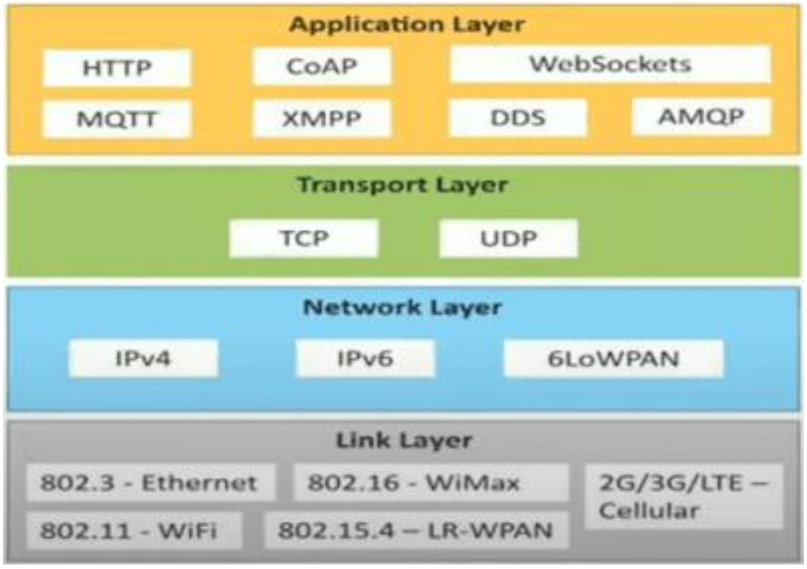
**Storage Interfaces**

Things like SD, MMC, and SDIO are used to store the data generated from an IoT device.

Other things like DDR and GPU are used to control the activity of an IoT system.

**IoT Protocols**

These protocols are used to establish communication between a node device and a server over the internet. it helps to send commands to an IoT device and receive data from an IoT device over the internet. we use different types of protocols that are present on both the server and client-side and these protocols are managed by network layers like application, transport, network, and link layer.




**Application Layer protocol**

In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface. these protocols include HTTP, WebSocket, XMPP, MQTT, DDS, and AMQP protocols.

**HTTP**

Hypertext transfer protocol is a protocol that presents in an application layer for transmitting media documents. it is used to communicate between web browsers and servers. it makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between two requests.

**WebSocket**

This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. this protocol is commonly used by web browsers.

**MQTT**

It is a machine-to-machine connectivity protocol that was designed as a publish/subscribe messaging transport. and it is used for remote locations where a small code footprint is required.

**Transport Layer protocol**

This layer is used to control the flow of data segments and handle the error control. also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

**TCP**

The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.

**UDP**

a user datagram protocol is a part of an internet protocol called the connectionless protocol. this protocol is not required to establish the connection to transfer data.

**Network Layer protocol**

This layer is used to send datagrams from the source network to the destination network. we use IPv4 and IPv6 protocols as host identification that transfers data in packets.

**IPv4**

This is a protocol address that is a unique and numerical label assigned to each device connected to the network. an IP address performs two main functions host and location addressing. IPv4 is an IP address that is 32-bit long.

**IPv6**

It is a successor of IPv4 that uses 128 bits for an IP address. it is developed by the IETF task force to deal with long-anticipated problems.

**Link Layer protocol**

Link-layer protocols are used to send data over the network's physical layer. it also determines how the packets are coded and signaled by the devices.

**Ethernet**

It is a set of technologies and protocols that are used primarily in LANs. it defines the physical layer and the medium access control for wired ethernet networks.

**WiFi**

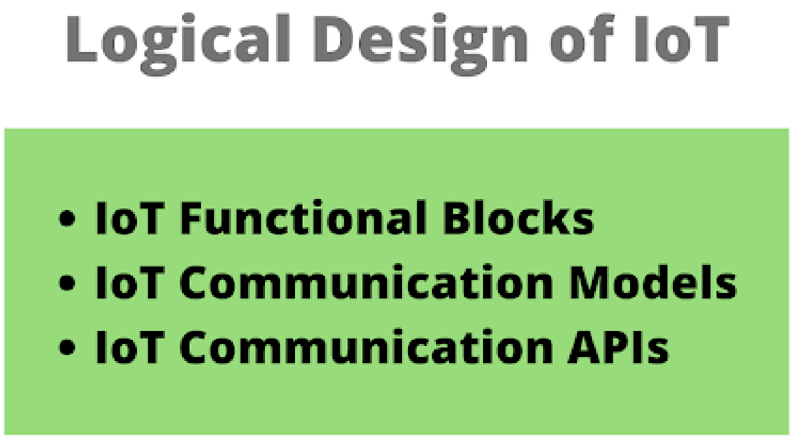
It is a set of LAN protocols and specifies the set of media access control and physical layer protocols for implementing wireless local area networks.

---

**Logical Design of IoT**

The logical design of an IoT system refers to an abstract representation of entities and processes without going into the low-level specifies of implementation. it uses Functional Blocks, Communication Models, and Communication APIs to implement a system.

But before you learn about the logical design of IoT systems you need to know a little bit about the physical design of IoT.

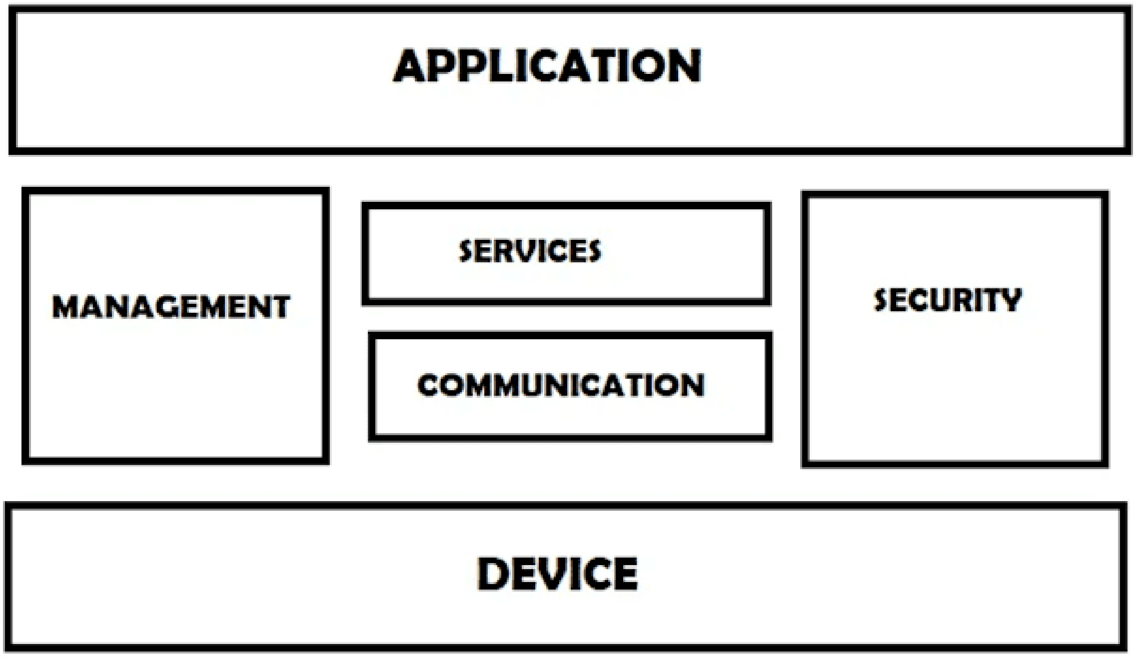



**Logical Design of Internet of Things(IoT)**

1. IoT Functional Blocks
2. IoT Communication Models
3. IoT Communication APIs

**IoT Functional blocks**

An IoT system consists of a number of functional blocks like Devices, services, communication, security, and application that provide the capability for sensing, actuation, identification, communication, and management.




These functional blocks consist of devices that provide monitoring control functions, handle communication between host and server, manage the transfer of data, secure the system using authentication and other functions, and interface to control and monitor various terms.

**Application**

It is an interface that provides a control system that use by users to view the status and analyze of system.

**Management**

This functional block provides various functions that are used to manage an IoT system.

**Services**

This functional block provides some services like monitoring and controlling a device and publishing and deleting the data and restoring the system.

**Communication**

This block handles the communication between the client and the cloud-based server and sends/receives the data using protocols.

**Security**

This block is used to secure an IoT system using some functions like authorization, data security, authentication, 2-step verification, etc.

**Device**

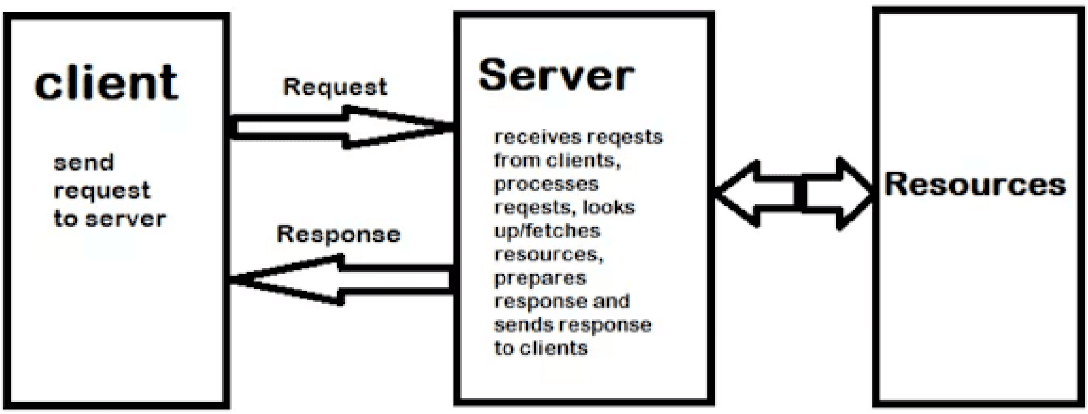
These devices are used to provide sensing and monitoring control functions that collect data from the outer environment.

**IoT Communication Models**

There are several different types of models available in an IoT system that is used to communicate between the system and server like the request-response model, publish-subscribe model, push-pull model, exclusive pair model, etc.

**Request-Response Communication Model**

This model is a communication model in which a client sends the request for data to the server and the server responds according to the request. when a server receives a request it fetches the data, retrieves the resources and prepares the response, and then sends the data back to the client.



Request-Response Communication Model

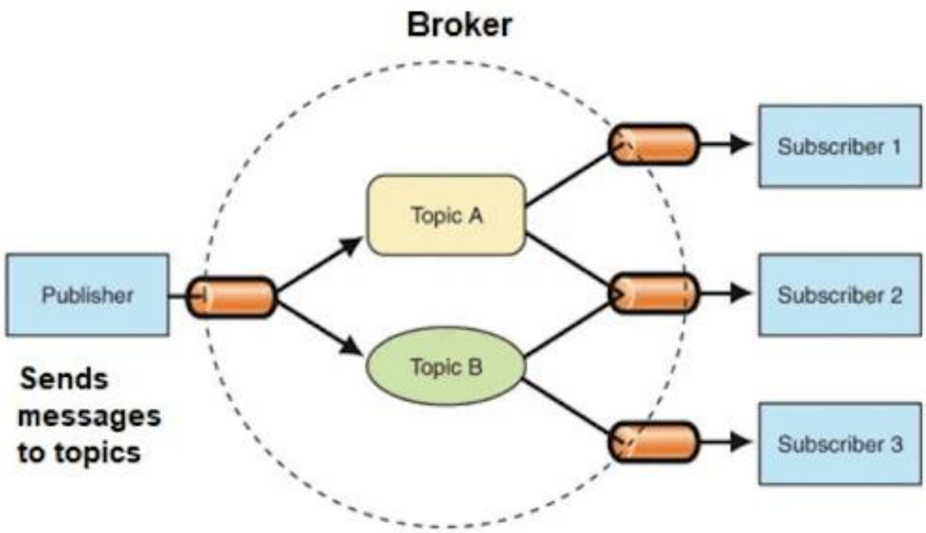
In simple terms, we can say that in the request-response model server send the response of equivalent to the request of the client. in this model, HTTP works as a request-response protocol between a client and server.

Example

When we search a query on a browser then the browser submits an HTTP request to the server and then the server returns a response to the browser(client).

**Publish-Subscribe Communication Model**

In this communication model, we have a broker between publisher and consumer. here publishers are the source of data but they are not aware of consumers. they send the data managed by the brokers and when a consumer subscribes to a topic that is managed by the broker and when the broker receives data from the publisher it sends the data to all the subscribed consumers.

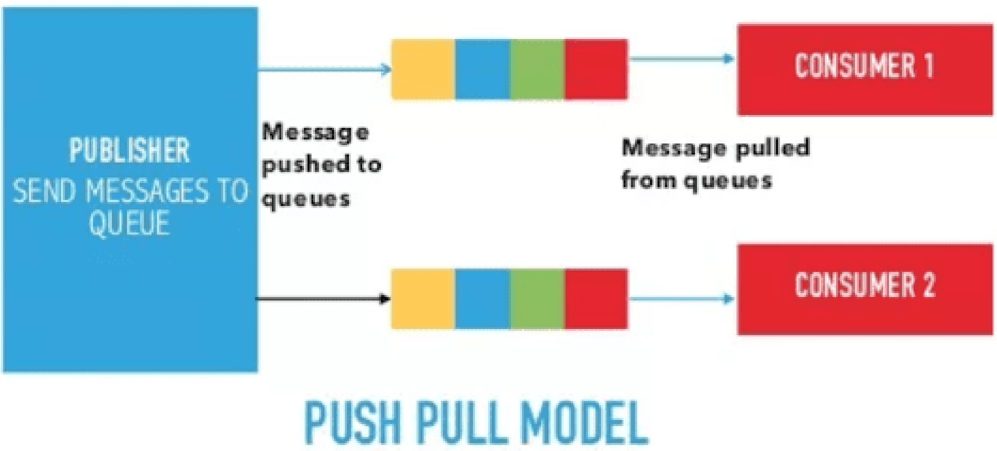



Example

On the website many times we subscribed to their newsletters using our email address. these email addresses are managed by some third-party services and when a new article is published on the website it is directly sent to the broker and then the broker sends these new data or posts to all the subscribers.

**Push-Pull Communication Model**

It is a communication model in which the data push by the producers in a queue and the consumers pull the data from the queues. here also producers are not aware of the consumers.



Example

When we visit a website we saw a number of posts that are published in a queue and according to our requirements, we click on a post and start reading it.

**Exclusive Pair Communication Model**

It is a bidirectional fully duplex communication model that uses a persistent connection between the client and server. here first set up a connection between the client and the server and remain open until the client sends a close connection request to the server.


**IoT communication APIs**

These APIs like REST and WebSocket are used to communicate between the server and system in IoT.

**REST-based communication APIs**

Representational state transfer(REST) API uses a set of architectural principles that used to design web services. these APIs focus on the systems' resources that how resource states are transferred using the request-response communication model. this API uses some architectural constraints.

**Client-server**

Here the client is not aware of the storage of data because it is concerned about the server and similarly the server should not be concerned about the user interface because it is a concern of the client. and this separation is needed for independent development and updating of server and client. no matter how the client is using the response of the server and no matter how the server is using the request of the client.

**Stateless**

It means each request from the client to the server must contain all the necessary information to understand by the server. because if the server can't understand the request of the client then it can't fetch the request data in a proper manner.

**Cacheable**

In response, if the cache constraints are given then a client can reuse that response in a later request. it improves the efficiency and scalability of the system without loading the extra data.

A RESTful web APIs is implemented using HTTP and REST principles.

**WebSocket based communication API**

This type of API allows bi-directional full-duplex communication between server and client using the exclusive pair communication model. this API uses full-duplex communication, so it does not require a new connection setup every time when it requests new data. WebSocket API begins with a connection setup between the server and client and if the WebSocket is supported by the server then it responds back to the client with the successful response after the setup of a connection server and the client can send data to each other in full-duplex mode.

this type of API reduces the traffic and latency of data and makes sure that each time when we request new data it cannot terminate the request.

---

# Questions:

1. **Define IOT. List its advantages, disadvantages, and applications**
2. **What are characteristics of IOT**
3. **Explain the architecture of IOT in detail**
4. **What are the challenges and issues in IOT system design?**
5. **Explain in detail about physical design of IOT**
6. **Explain in detail about Logical design of IOT**